(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 104 965 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.06.2001 Bulletin 2001/23

(51) Int Cl.[7]: **H04L 12/58**, H04M 3/533, G06F 17/60

(21) Application number: **99124151.4**

(22) Date of filing: **02.12.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Sony International (Europe) GmbH**
50829 Köln (DE)

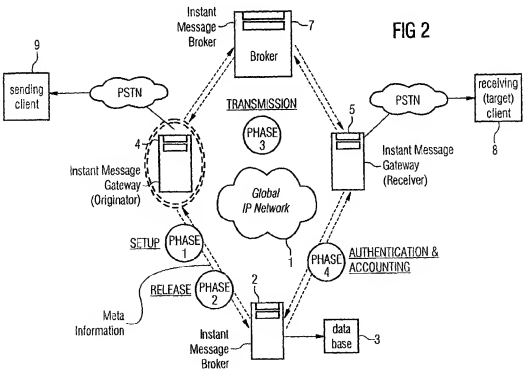
(72) Inventor: **Mache, Niels, Sony Int.(Europe) GmbH**
70736 Fellbach (DE)

(74) Representative: **Rupp, Christian, Dipl.Phys. et al**
Mitscherlich & Partner
Patent- und Rechtsanwälte
Sonnenstrasse 33
80331 München (DE)

(54) Protocol for instant messaging

(57) Messages are transmitted in nearly real-time in a distributed system. The message transmission system comprises a first message gateway (4) receiving a message from a sending client (9). Meta information is extracted by the first message gateway (4) from the received message and the meta information (MI) is transmitted from the first message gateway (4) to a message broker (2) connected to a client profile database (3). The message broker (2) selects a second message gateway (5) on the basis of the meta information and the client profile data of the client profile database (3). Than a message from the first message gateway (4) is transmitted to the selected second message gateway (5) which transfers the message to a target client (8).

FIG 2



EP 1 104 965 A1

Description

[0001] The present invention relates to a method for the transmission of messages in a distributed system, to a computer program product for implementing such a method in a network environment as well as to a distributed system for the transmission of messages.

[0002] The present invention generally relates to the field of electronic messaging. Electronic messages in the form of e-mails or GSM short message texts are known. They rely on a store-and-forward technique where the originator of the message sends the message to a computer node. In the node the message is stored and then forwarded to other nodes until it reaches a mailbox belonging to the intended user.

[0003] Also known from prior art are dedicated gateways for transferring a message from one transfer medium (e.g. SMS) to another transfer medium (e. g. fax). Several GSM network operators and independent service providers offer functionality like this. The major disadvantage of such systems is that there are targeted at a fixed transfer task, so is from one well-defined medium into another.

[0004] Another means known from prior art is the use of inexpensive intermediate networks for transmitting messages between different locations. For example, one could send a document as an attachment of a e-mail. This combined message is sent to dedicated gateway where it is converted to fax and transmitted to the intended recipient.

[0005] From US-A-5,608,786 an unified messaging system is known. This known technique makes use of existing communication channels or networks. Part of the system relies on a data communication network forming an intermediate leg of the distribution network. Telephone communication is typically used for initial or final legs. Voice mail, E-mail, facsimiles and other message types can be received by the system for retrieval by the subscriber. Communications may be centralised and retrieval of messages can be accomplished using one of a number of separate and distinct approaches. Thus, data communication networks such as the internet can become global voice mail and facsimile mail systems.

[0006] As state of the art messaging systems like e-mail have a store-and-forward-communication structure, they have inherently problems with instant (i. e. nearly real-time) message delivery.

[0007] Furthermore nearly real-time transmission of messages implies a big number of processing systems for high message throughput.

[0008] Therefore it is the object of the present invention to provide for a technique for the transmission of messages in a distributed system enabling for a high message throughput and a decreased load on the processing units of the distributed system.

[0009] Said object is achieved by means of the features of the independent claims. The dependent claims develop further the central idea of the present invention.

[0010] According to a first aspect of the present invention a method for the transmission of messages in a distributed system is provided. A message is received from a sending client by means of a first message gateway. Meta information extracted from the received message is transmitted from the first message gateway to a message broker. A second message gateway is selected on the basis of the meta information and client profile data. The message is sent from the first message gateway to the selected second message gateway to transfer it to a target client.

[0011] The message broker can process the meta information to provide for security and authentication and returns it to the first message gateway.

[0012] The message broker can process the meta information and return it to the first message gateway such that controlled by the processed meta information the message can be sent to the selected second gateway together with the meta information.

[0013] The message itself can be converted by a message processor before it is sent to the selected second message gateway.

[0014] According to another aspect the computer program product for implementing such a method in a network environment is provided.

[0015] According to still another aspect to the present invention a distributed system for the transmission of messages is provided. The system comprises a first message gateway for the reception of messages from sending clients and for the extraction of meta information from the received messages. A message broker receives the meta information from the first message gateway, processes the meta information and returns it to the first message gateway. The system furthermore comprises a second message gateway (which can be identical to the first message gateway) for receiving the message from the first message gateway controlled by the processed meta information and for sending the message to a target client.

[0016] A client profile database can be connected to the message broker. The message broker processes the meta information on the basis of the data of the client profile database.

[0017] The message broker can furthermore provide for a security and/or authentication functionality.

[0018] A message processor can be interconnected between the first and second message gateway for processing the content (and not the meta information) of a message.

[0019] Further features, advantages or objects of the present invention will be evident for the man skilled in the art when reading the following detailed description of embodiment of the present invention taken in conjunction with the figures of the enclosed drawings.

Fig. 1 shows an example of a instant messaging system,

Fig. 2 shows a communication structure of a messaging system,

Fig. 3 shows a message and information authentication protocol,

Fig. 4 shows a symmetric representation of the process according to the present invention, and

Fig. 5a and 5b show in detail a message and information authentication protocol.

[0020] Fig. 1 shows an example of a instant messaging system. The system essentially consists of instant message brokers 2 connected to client profile databases 3, gateways for e-mail 4, gateways for GSM/SMS 6, gateways for voice mail and facsimile 5 which can communicate with each other by means of a network 1. At least one message processor 7 can process particularly the content of transmitted messages. The instant message broker 2 manages the system configuration and state, user profiles of the client profile database 3, message routing and services, accounting and security.

[0021] Fig. 2 shows the communication structure of a messaging system. A configuration comprises an originator (instant message gateway 4), a receiver (instant message gateway 5) and a message broker 2 as well as additional units. The different units of such a system may be global distributed or located at a single computation node. In the example of Fig. 2 the data flow of such a minimal messaging system is schematically depicted.

[0022] In phase 1 the originator gateway 4 receives a message from a client (i. e. a facsimile from a PSTN), prepares (extracts) meta information from the message received and sends the meta information to the message broker 2.

[0023] In phase 2 the message broker 2 determines the required message conversion and the message route according to the state of the messaging system and client (sender and receiver) profiles stored in the connected database 3. Additionally the message broker 2 can prepare message security and also indication. The modified meta information is than returned from the instant message broker 2 to the originator gateway 4.

[0024] In phase 3 controlled by the meta information the originator gateway 4 transmits the instant message (consisting of meta information and message content) to the receiver gateway 5. In case where an additional message service or message conversion is required, the instant message can be routed over an additional message processor 7.

[0025] In phase 4 the receiver gateway 5 transmits the (eventually converted) message to the client. After transmission the receiver gateway 5 sends an acknowledgement (e. g. delivery, client receipt, or non-delivery) to the message broker 2, wherein the acknowledgement controls the message flow.

[0026] Fig. 3 shows in detail the message and information authentication protocol. At first in a set-up phase one the originator gateway 4 transmits meta information to the message broker 2, wherein the meta information can be signed.

[0027] In a release phase two the message broker 2 returns transmission management information (signed).

[0028] In a transmission phase three the originator gateway 4 transmits signed instant message to the receiver gateway 5 (optionally through message processors 7).

[0029] In a authentication and accounting phase four the receiver gateway 5 returns a signed acknowledgement to the message broker 2.

[0030] As reference to figure 4 the message transmission according to the present invention will be explained by means of the graphical representation.

[0031] In step S1 the originator gateway receives a message from a sending client. In a step S2 the originator gateway extracts meta information by performing a predetermined processing. In a step S3 a communication between the originator gateway and the message broker is set up and in a step S4 the meta information extracted in step S2 is transmitted. In step S5 the message broker modifies the meta information by using client profile data from connected client profile database. In step S6 the modified meta information (managing information) is transmitted from the message broker to the originator gateway. In step S7 a communication set-up between the originator gateway and a destination gateway is effected. In step S8 the message content and the meta information are transmitted from the originator gateway to the second (destination) gateway. In step S9 the message is delivered from the destination gateway to the target client. In step S10 the destination gateway returns a communication gateway to the message broker. In step S11 the message broker sends an acknowledgement to the originator gateway.

[0032] With reference to figure 4 the message and information authentication protocol will be explained in detail.

[0033] The originator gateway sends a time synchronised communication set-up (TSCS) login key to the instant message broker. The communication is set up by the transmission of the TSCS login key C and its digests HMAC (K1, C). The instant message broker checks the TSCS login key and returns a TSCS acknowledgement key containing a session key. The TSCS acknowledgement key containing the random generated session key C_{ack} is sent to the instant message gateway (originator). Note that the different session keys are randomly generated and unique for each communication step they are applied in.

[0034] The originator gateway appends the session key to the message and sends an instant message meta information (IMI) signed with the key K1 to the message broker. The instant message meta information (IMI) is transmitted with the appended session key C_{ack} and ist

digests HMAC (K1, IMI + C_{ack}). The message broker checks the instant message meta information (IMI) and inserts and modifies information in the IMI by using user profile tables and database information. The session key is appended to the message. The message is than signed with key K2 and key K1. The broker IMI is transmitted with the broker inner digest ID (corresponding to HMAC (K2, IMI + C_{ack}). The IMI in the broker digest are signed again with key K1 (outer digest HMAC (K1, IMI + C_{ack} + HMAC (K2, IMI + C_{ack})).

[0035] The originator gateway checks the outer digest and sends an acknowledgement process broker IMI to the message broker.

[0036] Than the originator gateway set ups a communication by the transmission of the TSCS login key C and its digest HMAC (K1, C) to the message gateway (destination). The destination gateway checks the TSCS login key and returns a TSCS acknowledgement key containing a session key. Therefore the TSCS acknowledgement key containing the session key C_{ack} is sent to the originator gateway.

[0037] The originator gateway appends the session key to the message and sends an instant message signed with key K1 to the destination gateway. Therefore an instant message (IM)(i. e. message data and IMI) containing the message M is transmitted to the destination gateway.

[0038] The destination gateway checks the instant message, converts the instant message and sends an acknowledgement which is signed to the originator gateway. The session is than finished for the originator gateway.

[0039] The message is than delivered from the destination gateway to the target client (customer).

[0040] The destination gateway is than sending a TSCS login key for a communication set-up to the message broker.

[0041] The message broker checks the TSCS login key and returns a TSCS acknowledgement key containing a session key to the destination gateway. In the acknowledgement step the destination gateway returns the broker ID (generated previously by the message broker) and a message delivery read acknowledgement and signs it with the key K1.

[0042] The destination gateway sends a broker IMI, message delivery/read acknowledgement and signs it with K1.

[0043] The message broker checks the outer digest generated by the destination gateway with the key K1, checks the returned ID by comparing it with its own (stored) previously generated ID sent to the destination gateway. processes the acknowledgement, terminates the transaction and returns the acknowledgement to the destination gateway.

[0044] The instant message meta information integrity and origin is assured by the generation of the meta information inner digest ID (by using the message broker key K2) and the comparison with the inner digest ID received from the destination gateway. Therefore the message broker can positively control the proper transmission of the inner digest ID from the sending gateway to the destination gateway. Furthermore it can be assured that no communication between the sending gateway and the destination gateway is possible without intervention of the message broker.

[0045] The message broker then sends a TSCS login key for a communication set-up to the originator gateway.

[0046] The originator gateway checks the digest, processes the acknowledgement, notifies the sending client and returns an acknowledgement to the message broker.

[0047] The message broker than transmits a transmission message delivery acknowledgement signed with K1 to the originator gateway.

[0048] The originator gateway checks the TSCS login co-key and returns a TSCS acknowledgement key containing the session key to the instant message broker.

[0049] The invention therefore provides a technique for (nearly) real-time capital flow control of direct messaging in a distributed messaging system.

[0050] The purpose of instant messaging is to transmit high priority messages in (nearly) real-time between clients (man and machine). Unified messaging merges analog and digital transmitted messages such as facsimile, voice mail, e-mail, WWW and the cell phone short message service (GSM/SMS) to unified instant messages. A Unified Instant Messaging System (UIMS) is a (global) distributed system that consists of four major components that communicate with each other over an IP network: distributed gateways, message processors message brokers and a client directory database. Messages of arbitrary form are converted into Unified Instant Messages by the Instant Message Gateways and vice versa. The Instant Message Brokers (IMB) controls the message flow, accounting and message conversion Additionally message brokers must ensure the authentication and security of instant messages to prevent the distributed system from unauthorised access.

[0051] The present invention is an efficient data transmission protocol for the transmission of messages in nearly real-time. In an UIMS a relatively small number of message brokers manages the message transfer, processing and security. Thus, the communication protocol and unified message structure is optimised for high message throughput and a minimum broker load. Instead of complete message transmission and processing, IMBs processes message meta information.

[0052] The present invention describes an apparatus and method for controlling message flow and processing in a distributed instant (i.e. nearly real-time) messaging systems. Because of the meta information is much more compact as the message itself, a higher throughput with reduced data transfer is reached. The (meta) message content and control flow is transmitted with authentication which means that it allows the communicat-

ing parties (gateways processors and brokers) to verify that the received messages (as well as the true and alleged originator) are authentic. In MIAP information is authenticated using Time Synchronised Communication Setup by Keyed-Hashing Message Authentication (TSCS) for message authentication.

[0053] Authenticated, high throughput apparatus and method (protocol) for a communication in distributed, direct messaging systems are proposed. The message flow control and further messaging process of such a system is managed by one of several instances of message brokers. Time synchronised communication set up by keyed-hashing method authentication (TSCS) for message authentication is used.

Claims

1. Method for the transmission of messages in a distributed system, the method comprising the following steps:

   - reception of a message from a sending client (9) by a first message gateway (4),
   - transmission of meta information extracted from the received message from the first message gateway (4) to a message broker (2),
   - selection of a second message gateway (5) on the basis of the meta information and client profile data (3), and
   - sending the message from the first message gateway (4) to the selected second message gateway (5) to transfer it to a target client (8).

2. Method according to claim 1,
   characterized in that
   the message broker (2) processes the meta information to provide for security and authentication and returns it to the first message gateway (4).

3. Method according to anyone of the preceding claims,
   characterized in that
   the message broker (2) processes the meta information and returns it to the first message gateway (4) and in that, controlled by the processed meta information, the message is sent to the selected second gateway (5) together with the meta information.

4. Method according to anyone of the preceding claims,
   characterized in that
   the message itself is converted by a message processor (7) before it is sent to the selected second message gateway (5).

5. Computer program product,
   characterized in that
   it implements a method according to anyone of the preceding claims when loaded in the memory of a computing device in a network environment.

6. Distributed system for the transmission of messages, the system comprising:

   - a first message gateway (4) for the reception of messages from sending clients (9) and for the extraction of meta information from the received messages,
   - a message broker (2) for receiving the meta information from the first message gateway (4), processing the meta information and returning it to the first message gateway (4), and
   - a second message gateway (5) for receiving the message from the first message gateway (4) controlled by the processed meta information and for sending the message to a target client (8).

7. Distributed system according to claim 6,
   characterized by
   a client profile database (3) connected to the message broker (2), wherein the message broker (2) processes the meta information on the basis of the data of the client profile database (3).

8. Distributed system according to anyone of claims 6 or 7,
   characterized in that
   the message broker (2) provides for a security and/or authentication functionality.

9. Distributed system according to anyone of claims 6 to 8,
   characterized by
   a message processor (7) interconnected between the first and second message gateway (4, 5) for processing the content of the message.

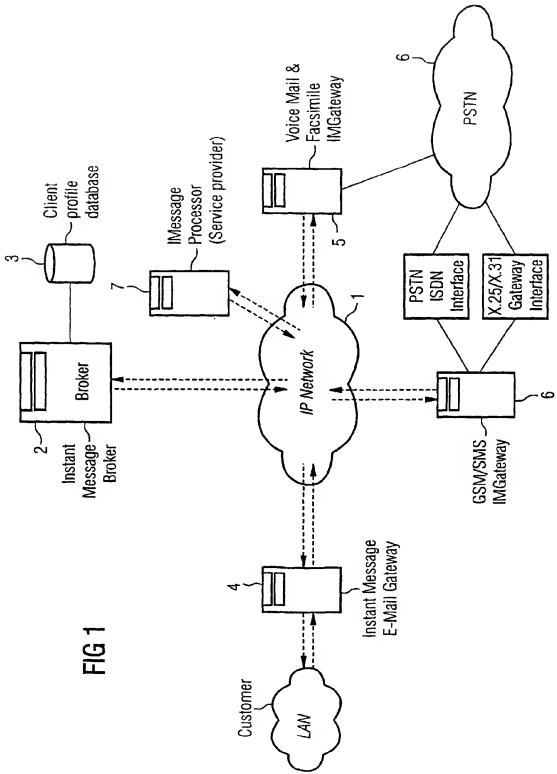

Customer
LAN
4
Instant Message
E-Mail Gateway
Instant
Message
Broker
2
Broker
3
Client
profile
database
IP Network
1
IMessage
Processor
(Service provider)
7
Voice Mail &
Facsimile
IMGateway
5
6
PSTN
PSTN
ISDN
Interface
X.25/X.31
Gateway
Interface
GSM/SMS
IMGateway
6

FIG 1

FIG 2

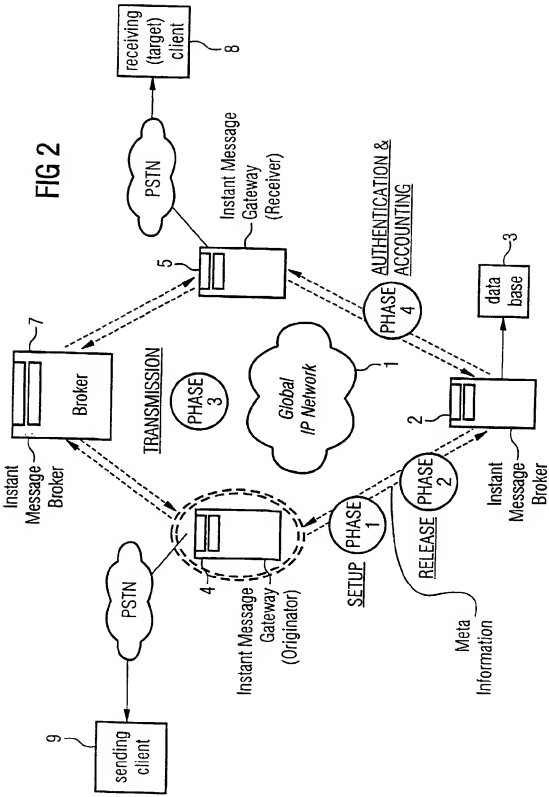

receiving (target) client
8
PSTN
Instant Message Gateway (Receiver)
5
7
Broker
Instant Message Broker
TRANSMISSION
PHASE 3
Global IP Network
1
PHASE 4
AUTHENTICATION & ACCOUNTING
data base
3
2
Instant Message Broker
PHASE 2
RELEASE
Meta Information
PHASE 1
SETUP
4
Instant Message Gateway (Originator)
PSTN
9
sending client

FIG 3

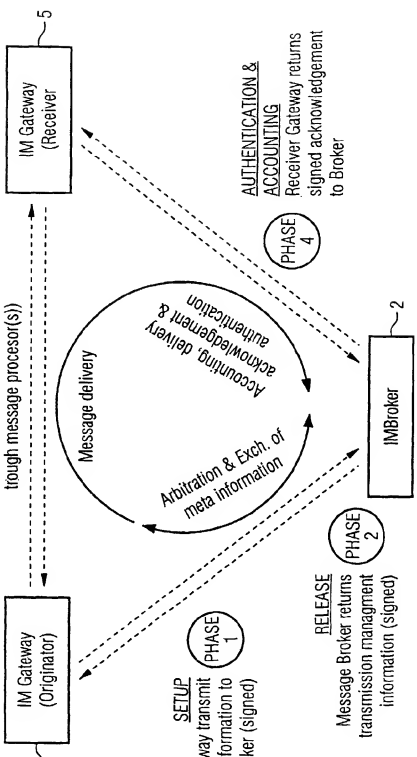
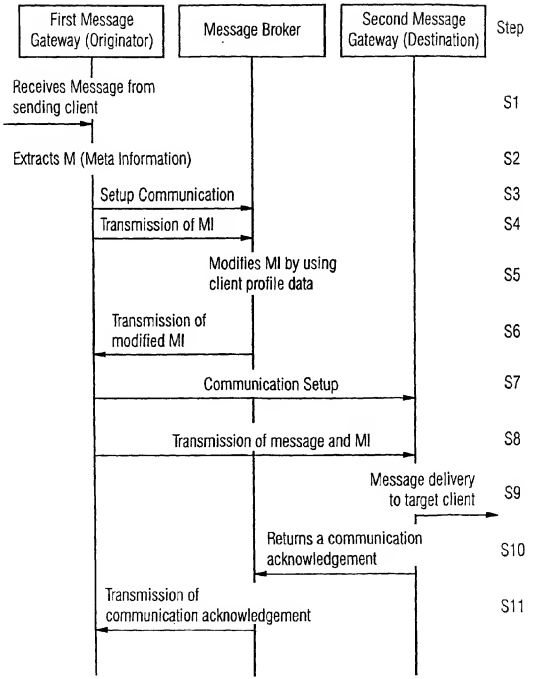

IM Gateway (Originator)
4
IM Gateway (Receiver
5
IMBroker
2
PHASE 1
SETUP
Gateway transmit meta information to Message Broker (signed)
PHASE 2
RELEASE
Message Broker returns transmission managment information (signed)
PHASE 3
TRANSMISSION
Originator Gateway transmits signed instant message to receiver gateway (optional trough message procesor(s))
PHASE 4
AUTHENTICATION & ACCOUNTING
Receiver Gateway returns signed acknowledgement to Broker
Message delivery
Arbitration & Exch. of meta information
Accounting, delivery acknowledgement & authentication

FIG 4


First Message Gateway (Originator)
Message Broker
Second Message Gateway (Destination)
Step
Receives Message from sending client
S1
Extracts M (Meta Information)
S2
Setup Communication
S3
Transmission of MI
S4
Modifies MI by using client profile data
S5
Transmission of modified MI
S6
Communication Setup
S7
Transmission of message and MI
S8
Message delivery to target client
S9
Returns a communication acknowledgement
S10
Transmission of communication acknowledgement
S11

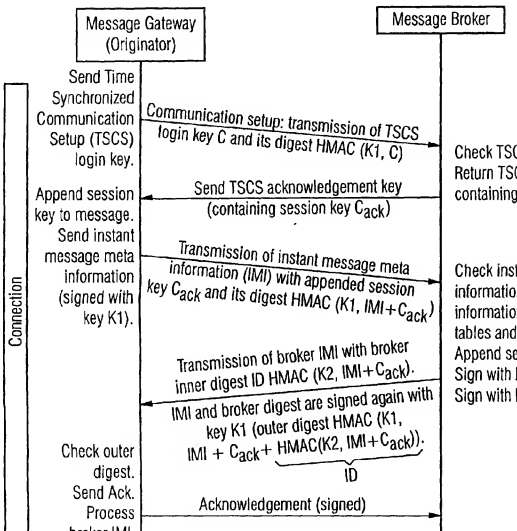

Message Gateway (Originator)
Message Broker
Connection
Send Time Synchronized Communication Setup (TSCS) login key.
Communication setup: transmission of TSCS login key C and its digest HMAC (K1, C)
Check TSCS login key.
Return TSCS ackowledgement key containing session key.
Append session key to message.
Send TSCS acknowledgement key (containing session key C_{ack})
Send instant message meta information (signed with key K1).
Transmission of instant message meta information (IMI) with appended session key C_{ack} and its digest HMAC (K1, IMI+C_{ack})
Check instant message meta information (IMI). Insert and modify information in IMI by using user profile tables and database information.
Append session key to message.
Sign with key K2
Sign with key K1
Transmission of broker IMI with broker inner digest ID HMAC (K2, IMI+C_{ack}).
IMI and broker digest are signed again with key K1 (outer digest HMAC (K1, IMI + C_{ack}+ HMAC(K2, IMI+C_{ack})).
ID
Check outer digest.
Send Ack.
Process broker IMI.
Acknowledgement (signed)

FIG 5 A

FIG 5 B

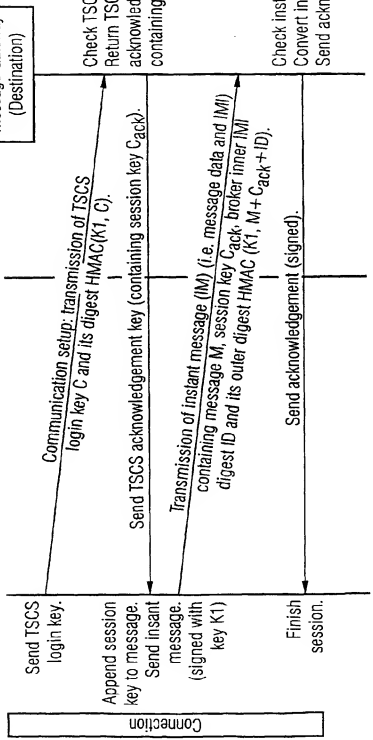

Connection
Message Gateway (Destination)
Send TSCS login key.
Communication setup: transmission of TSCS login key C and its digest HMAC(K1, C).
Check TSCS login key.
Return TSCS acknowledgement key containing session key.
Append session key to message.
Send insant message. (signed with key K1)
Send TSCS acknowledgement key (containing session key Cack).
Transmission of instant message IM) (i.e. message data and IMI) containing message M, session key Cack, broker inner IMI digest ID and its outer digest HMAC (K1, M+Cack+ID).
Check instant message.
Convert instant message.
Send acknowledgement.
Finish session.
Send acknowledgement (signed).

FIG 5 C

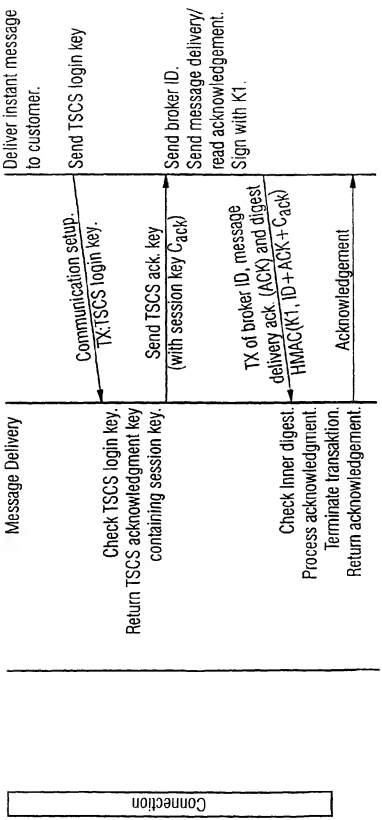
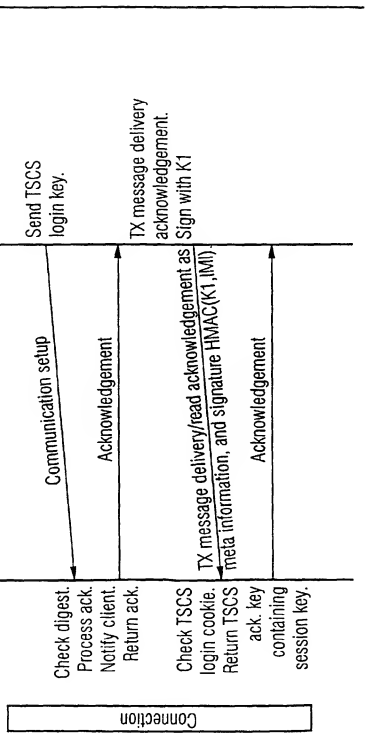

Connection
Message Delivery
Deliver instant message to customer.
Communication setup.
TX:TSCS login key.
Send TSCS login key
Check TSCS login key.
Return TSCS acknowledgment key containing session key.
Send TSCS ack. key (with session key C_{ack})
Send broker ID.
Send message delivery/ read acknowledgement.
Sign with K1.
TX of broker ID, message delivery ack. (ACK) and digest HMAC(K1, ID+ACK+C_{ack})
Check Inner digest.
Process acknowledgment.
Terminate transaktion.
Return acknowledgement.
Acknowledgement

FIG 5 D


Connection
Check digest.
Process ack.
Notify client.
Return ack.
Communication setup
Send TSCS
login key.
Acknowledgement
TX message delivery
acknowledgement.
Sign with K1
Check TSCS
login cookie.
Return TSCS
ack. key
containing
session key.
TX message delivery/read acknowledgement as
meta information, and signature HMAC(K1,IMI).
Acknowledgement

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 12 4151

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 742 905 A (BROCKMAN JAMES JOSEPH ET AL) 21 April 1998 (1998-04-21) * abstract * * column 3, line 10 - line 58 * * column 5, line 56 - column 8, line 30 * * column 19, line 65 - column 20, line 25 * * column 23, line 12 - column 24, line 53 * * column 29, line 26 - column 30, line 13 * * column 36, line 52 - line 59 * ---	1-9	H04L12/58 H04M3/533 G06F17/60
A	US 5 740 230 A (VAUDREUIL GREGORY M) 14 April 1998 (1998-04-14) * abstract * * column 3, line 60 - column 8, line 64 * * column 19, line 49 - column 20, line 53 * * column 21, line 40 - column 22, line 41 * * column 24, line 24 - column 25, line 3 * * column 28, line 61 - column 29, line 41 * * figures 1-3,11-14 * ---	1,6	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L H04M G06F
A	WO 98 58491 A (CRANBERRY PROPERTIES LLC) 23 December 1998 (1998-12-23) * abstract * * page 3, line 1 - line 24 * * page 6, line 3 - page 8, line 13 * * page 11, line 19 - page 12, line 12 * * figures 1,2 * ---	1,6	
A	US 5 608 786 A (GORDON ALASTAIR T) 4 March 1997 (1997-03-04) * abstract * * column 1, line 66 - column 3, line 64 * ------	1,6	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	10 May 2000	Poggio, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 12 4151

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information

10-05-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5742905 A	21-04-1998	CA 2199802 A	28-03-1996
		EP 0782805 A	09-07-1997
		JP 9511884 T	25-11-1997
		WO 9609714 A	28-03-1996
		US 5742668 A	21-04-1998
US 5740230 A	14-04-1998	NONE	
WO 9858491 A	23-12-1998	US 6023700 A	08-02-2000
		AU 7971298 A	04-01-1999
US 5608786 A	04-03-1997	CA 2139081 A	24-06-1996
		AU 4294996 A	19-07-1996
		WO 9620553 A	04-07-1996
		CN 1173260 A	11-02-1998
		EP 0799543 A	08-10-1997
		JP 10511823 T	10-11-1998
		NZ 297714 A	28-01-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No 12/82